Europäische Datenschutz-Grundverordnung (DS-GVO)

Clara Fritsch, Abteilung Arbeit & Technik

Innsbruck, 12. und 13. Oktober 2017

Grundrechte

- ***„Jeder Mensch hat angeborne, schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten.“***
  (§ 16 ABGB; seit 1.1.1812)

- **„…an employer’s instructions cannot reduce private social life in the workplace to zero.** Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.”
  (EUGH am 5.9.2017)

Grundrechte (2)

- **Grundrecht auf Achtung des Privat- und Familienlebens**
  (Art 8 MRK)
  → zB Videoüberwachung f. Privatsphäre grundsätzlich verboten (DSG + DSAG)
- **Grundrecht auf Information**
  (Art 11 EChM)
  → zB Nutzung von Telefon (OGH) {anderen Kommunikationsmitteln}
- **Schutz personenbezogener Daten**
  (Art 8 EChM)

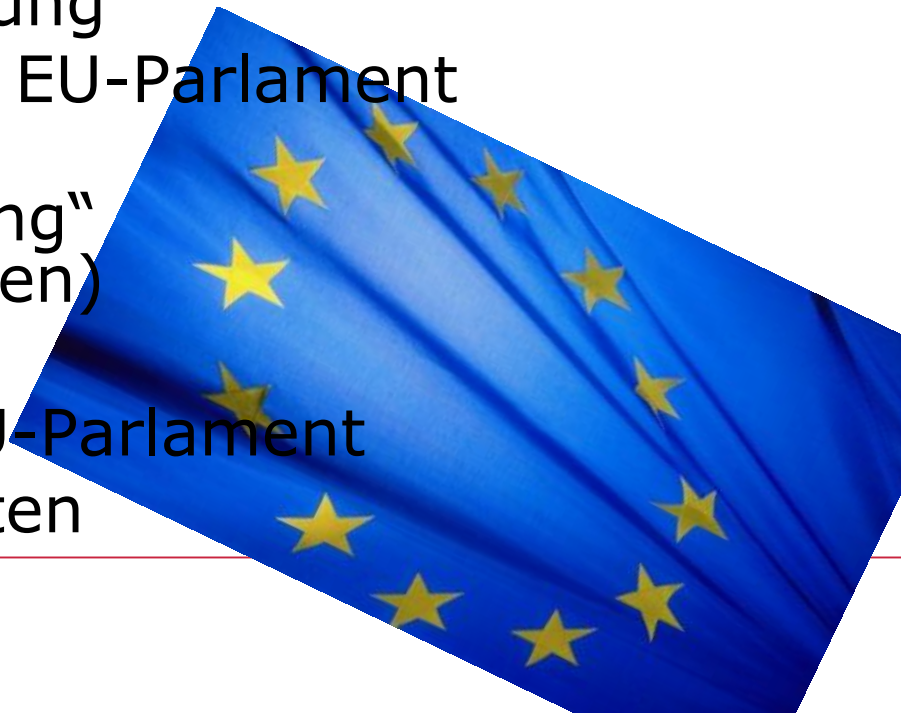
personenbezogene Daten im Betrieb

- Bild
- Ton
- Text
- Zeit
- Stammdaten
- Einkommen
- Qualifikation
- Gesundheit
- Gespräche
- Ortung
- Protokolle, Akten
- Logfiles
- Leistung und Verhalten
- Zutritt

„*alle Informationen die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; … direkt oder indirekt, mittels Zuordnung zu einer Kennung*“ (Art 4 Z 1 DSGVO)

Werdegang der europäischen Datenschutzgesetzgebung

- 1990: Vorschlag für eine EU-Richtlinie
- 1995: Inkrafttreten der EU-Richtlinie
- 2010: EU-Konsultation zur Novellierung
- Jän. 2012: Vorschlag der EU-Kommission für eine Datenschutz-Grundverordnung
- Okt. 2013: Abstimmung im EU-Parlament
  4.000+ Änderungsanträge
- Juni 2015: EU-Rats-"Einigung"
  (ohne Österreich + Slowenien)
- Jän. 2016: Trilog-Einigung
- April 2016: Annahme im EU-Parlament
- **25. Mai 2018**: Inkraft-Treten



Werdegang der österreichischen Datenschutzgesetzgebung

- 1980: erstes österr. DSG
- 1998: Ende der Frist für die Umsetzung der EU-Richtlinie in nationales Recht
- Jänner 2000: DSG 2000 tritt in Kraft
- März 2005: DSG-Novelle (Datenweitergabe im Katastrophenfall + erweitertes SicherheitspolizeiG)
- Jänner 2010: Novelle des DSG 2000 (Video)
- Jänner 2014: Novelle des DSG 2000 (Verwaltungsreform)
- Juni 2017 Datenschutz-Anpassungsgesetz

… und was hat eigentlich die GPA-djp gemacht?

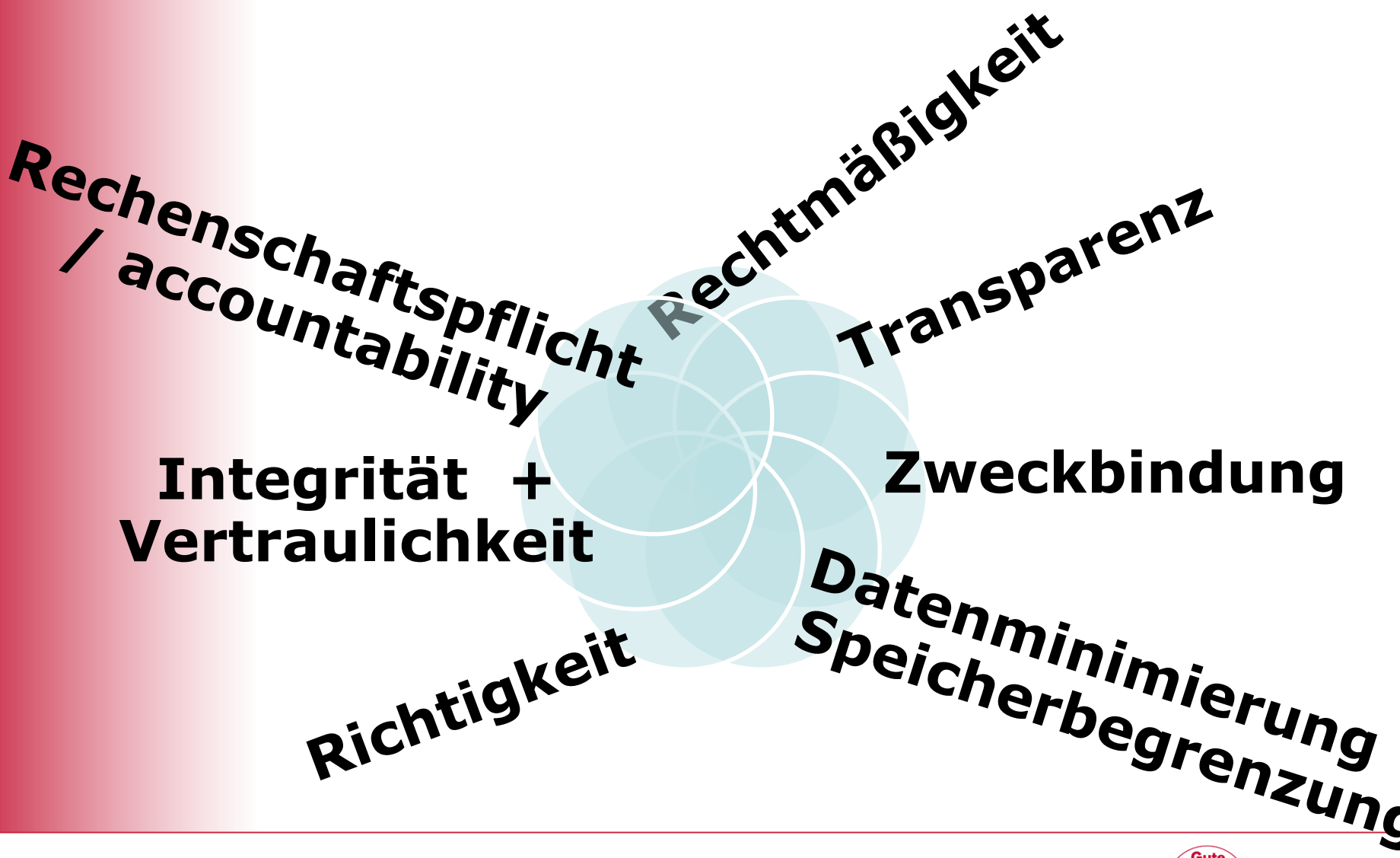
- Jänner 2010: ÖGB-Stellungnahme zur KOM-Konsultation
- Stellungnahme des EWSA zur KOM-Konsultation
- Oktober 2010: Antrag zum Datenschutz am Bundesforum
- Juni 2011: Stellungnahme EWSA zum Schutz personenbezogener Daten
- Parlamentarische Anfrage Weidenholzer/ Regner
- Lobbying bei KOM Nemietz (Koop verdi, AK)
- März 2012: Brief Katzian → Hundstorfer
- Brief ÖGB Foglar → BKA
- ÖGB Stellungnahme zu DSGVO-Entwurf
- April 2012: Veranstaltung (Koop AK, MEPs, verdi)
- Mai 2012: EWSA-Stellungnahme zur DSGVO
- September 2012: Lobbying in Brüssel bei EGB, MEPs, bei sämtlichen Bericht- und SchattenberichterstatterInnen aller Fraktionen
- Oktober 2012: EGB-Positionierung zur DSGVO
- Dezember 2012 - Februar 2013: Lobbying der EMPL-Änderungsanträge

… und was hat eigentlich die GPA-djp gemacht? (Teil 2)

- Februar 2013: ExpertInnen Hearing am round table im EP (AK, DGB, Wirtschaft,…)
- Juni 2013: Presseaussendung Katzian – u.a. zu Stärkung der Behörde
- Jänner 2014: Grundrechte-Konferenz (Koop AK)
- Oktober 2014: Brief Katzian → Hesse
- Jänner 2015: internationaler Beitrag (zum betr. DSB) in CPDP-Publikation (Springer Verlag) zum DSB
- September 2015: Foglar+Kaske Brief zur Gefährdung der Mitbestimmung → Trilog-Verhandler + BKA
- Jänner 2016: Kompetenz-Artikel (m. Lucia Bauer)
- April 2016: VA zu DSGVO (Koop mit RI und AK)
- Juli 2016: Brief Katzian → Kern + Stöger

- laufend Beratungen/ Referate/ Seminare/ Blog-Beiträge/ Artikel in der Kompetenz und anderswo @ DSGVO

Grundsätze des Datenschutzes



Who is who and what is what?

DSG	DSGVO	ArbVG
Betroffene	Betroffene	ArbeitnehmerIn
Auftraggeber	VerantwortlicheR	BetriebsinhaberIn
Dienstleister	Auftragsdaten-verarbeiter	
		Betriebsrat • Mitbestimmung • Veto • Kontrolle • Information • Beratung
Datenschutzkommission / Datenschutzbehörde	Unabhängige Aufsichtsbehörde	
Artikel-29-Datenschutzgruppe	Europäischer Datenschutzausschuss	

vorher - nachher

DS-Richtlinie und DSG 2000	DSGVO ab 25.5.2018
Richtlinie	Verordnung + Marktortprinzip
Meldepflicht beim Datenverarbeitungsregister (DVR)	Verfahrensverzeichnis (Art. 30) und Datenschutzfolgenabschätzung (Art. 35f)
Sanktionen jetzt	Sanktionen verschärft (Art. 83f)
___	Betrieblicher Datenschutzbeauftragter (Art. 37ff)
§ 9 Z 11, § 50a Abs 5, § 14 Abs 4 DSG 2000	Beschäftigten-Datenschutz (Art. 88)
Mitbestimmung im ArbVG	Mitbestimmung im ArbVG

Betroffenenrechte (Art 17-22)

- Auskunftsrecht
- Recht auf Berichtigung und Löschung („Recht auf Vergessenwerden“)
- Widerspruchsrecht
- Verbot von automatisierten Einzelentscheidungen („Profiling“)
- *Recht auf Einschränkung der Verarbeitung*
- *Recht auf Datenübertragbarkeit*
- + umfassende Informationspflichten des Verantwortlichen (Art 13-15)

Sanktionen

DSG 2000

- vorsätzlich, widerrechtliche Datenverwendung
  (zB Zugang, Übermittlung, Zweckentfremdung)
  → bis zu 25.000 EUR
- Verstöße gegen DSG
  (zB Melde-, Informations-, Genehmigungspflicht, keine Sicherheitsmaßnahmen,…)
  → bis zu 10.000 EUR
- immer pro Einzelfall
- *quasi totes Recht*

DSGVO

- Haftung für materielle und immaterielle Schäden vom Verantwortlichen *und* Auftragsverarbeiter
- Recht auf Schadenersatz
- → bis 20 Mio EUR bzw **4%** des gesamten weltweit erzielten Umsatzes

DatenschutzbeauftragteR

- Verpflichtend einzuführen wenn
  - Behörde
  - Kerntätigkeit eine umfangreiche Datenverarbeitung mit regelmäßiger und systematischer Beobachtung von Personen umfasst
  - Kerntätigkeit besondere Kategorien von Daten umfasst
- Öffnungsklausel zur *Bestellung*
- innerbetrieblich oder extern
- Unterrichtung und Beratung
- Überwachung der DSGVO
- Sensibilisierung und Schulung
- Ansprechpartner für Behörde
- berufliche Qualifikation und Fachwissen erforderlich
- Wahrung der Geheimhaltung und Vertraulichkeit
- Mitarbeit bei der Datenschutzfolgenabschätzung und (allfälliger) Vorab-Konsultation

Einwilligung

- Beweislastumkehr (AG muss beweisen)
- eindeutig
- verständlich
- freiwillig
- Widerrufsrecht

Löschung

- „Recht auf Vergessenwerden“
- „Recht auf Einschränkung der Verarbeitung“
- AUCH bei Veröffentlichung/ Übermittlung/ etc.

Auskunft

- Zweck
- Kategorien
- Empfänger
- *Dauer*
- Beschwerderecht bei Behörde
- (wenn profiling): Logik, Tragweite, dahinter, angestrebte Auswirkungen
- (wenn nicht direkt erhoben): Herkunft
- (wenn in ein Drittland übermittelt): Garantie über Sicherheit dort

Datenschutz durch Technik

- „privacy by design“ & „privacy by default“
- technische und organisatorische Maßnahmen, zB Pseudonymisierung
- Voreinstellung in Produkten, um Zweckbindung und Datensparsamkeit zu gewährleisten
- Konzepte zum Löschen
- Zugriffseinstellungen
- Zertifizierungsverfahren als Nachweis möglich

Verarbeitungsverzeichnis

- wenn >250 MA
- wenn Risiko für Rechte von Personen
- wenn Profiling
- wenn besondere Datenkategorien umfangreich verarbeitet werden
- wenn strafrechtlich Relevantes
- Inhalte: Name, Zweck, Kategorien, Empfänger, *Löschfristen*, Sicherheitsmaßnahmen
- Muss der Behörde vorgelegt werden

Folgenabschätzung

- wenn Risiko für Rechte von Personen
- wenn Profiling
- wenn besondere Datenkategorien umfangreich verarbeitet werden
- wenn öffentlicher Bereich überwacht wird
- Rat des betriebl. DSB
- MUSS-Inhalte: Zweck, Notwendigkeit, Verhältnismäßigkeit, Risikobewertung, geplante Abhilfe
- bei Risiko → Vorab-Konsultation der Behörde
- Behörde muss Auskunft erhalten
- Behörde wird **Whitelist & Blacklist** erstellen

Grundlagen f Datenverarbeitung im Konzern

- **Verhaltensregeln** f. Unternehmen/ Branchen (Art. 40f)
  - freiwillige Selbstverpflichtung
  - selbst erarbeitet
  - Genehmigung durch DS-Behörde
  - Veröffentlichung
- **Zertifizierung** (Art. 42f)
  - DS-Behörde akkreditiert eigene Zertifizierungsorganisationen
- **interne Datenschutzvorschriften** f. Konzerne (Art. 47)
  - enthalten durchsetzbare Rechte für Betroffene
  - Genehmigung durch DS-Behörde
  - Schulungen für Personal verpflichtend

„One-stop-shop"

- Verantwortlicher für DS in EU muss benannt werden
- Hauptniederlassung muss benannt werden
- Aufsichtsbehörde der Hauptniederlassung in allfälligen Auseiandersetzugnen federführend (Art 56)
- Behörde im jeweils betroffenen Mitgliedstaat hat Überwachungsbefugnisse (Art 57-58)
- Enge Zusammenarbeit zwischen den Behörden geboten (Art 60-62)
- Kohärenzverfahren zur einheitlichen Rechtsanwendung (Art 63-67)

weitere Neuerungen in der DSGVO

- Einwilligung bei Kindern geklärt (Art. 8)
- Kohärenz und Zusammenarbeit der DS-Behörden (Art. 60 ff)
- „Verbandsklage light“ Vertretung von Betroffenen für Datenschutz-Organisationen & Vereine (Art. 80)
- Beschäftigten-Datenschutz (Art. 88) mit Öffnungsklausel

Das österreichische DSG

- **BR-Rechte bleiben unberührt (§ 11)**
- Regelungen zur Videokontrolle ergänzt um akustische Aufnahmen
  - Verboten zum Zwecke der Mitarbeiterkontrolle (§ 12 Abs 2)
  - Verbot an „höchstpersönlichen" Orten (§ 12 Abs 4 Z 1)
  - Aufbewahrungsdauer 72 Stunden (§ 13 Abs 3)
  - Kennzeichnungspflicht f. überwachten Bereich (§ 13 Abs 5)
- Online-Registrierungsverfahren fällt weg → Vorab-Kontrolle fällt weg
- Kein ausdifferenzierter Beschäftigten-Datenschutz
- Kein richtiges Verbandsklagerecht
- Keine Mitbestimmung des BR bei der Bestellung des betr. Datenschutzbeauftragten

Was gibt es Neues?

- Richtlinie → Verordnung mit Marktortprinzip
- Hauptniederlassung (one-stop-shop)
- DatenschutzbeauftragteR
- Behördenkooperation
- DVR → betriebliches Verarbeitungsregister
- Datenportabilität
- Datenschutzfolgenabschätzg
- Zertifizierung u.a.
- DP by design/ default
- Beschäftigtendatenschutz
- „Verbandsklagerecht light"
- **erhöhter Strafrahmen**

Was bleibt beim Alten?

- Grundprinzipien
- Verbot von Profiling
- Sensible Daten → besondere Kategorien (inkl. biometrische + genetische Daten)
- Artikel-29-Arbeitsgruppe → Europ. DS-Ausschuss

- **Nationales Mitbestimmungsrecht!**

Der OGH sagt:

- *Ein **elektronisches Telefonsystem** ist zustimmungspflichtig gemäß §96 ArbVG (OGH 13.6.2002, 8 ObA 288/01p)*

- *Es besteht ein **umfängliches Informationsrechts** des BR gemäß § 91 ArbVG [jedoch keine BV-Pflicht gemäß §96a ArbVG] „Mystery Flyers" (OGH 22.10.2010, 9 ObA 135/09g)*

Der OGH sagt (2):

- ***Personalfragebögen**, die nur allgemeine, einzelnen AN nicht zuordenbare Ergebnisse beinhalten, sind nicht an die Zustimmung des BR zu binden (OGH 15.12.2004, 9 ObA 114/04m)*
- *Ein **Fingerscan-System zur Zeiterfassung** ist NICHT zulässig (OGH 20.12.2006, 9 ObA 109/06d)*
- *Unangekündigte verdachtsunabhängige **Alkoholkontrollen** durch Alkomaten sind zustimmungspflichtig (OGH 20.3.2015, 9 ObA 23/15w)*

Inhalte von Betriebsvereinbarungen

- Zielsetzung bzw. Verwendungszweck
- Welche personenbezogenen Daten werden ermittelt?
- Welche personenbezogenen Auswertungen werden gemacht?
- Welche personenbezogenen Daten werden an weitere Empfänger weitergegeben und zu welchen Zwecken?
- Wann werden die Daten gelöscht?
- Informations-, Mitbestimmungs- und Kontrollrechte des BR
- Rechte der ArbeitnehmerInnen
- Systembeschreibung als Bestandteil der BV

Kennzeichen einer guten DS-Regelung

- **Beschränkung des Zweckes**
- **Beschränkung der Quantität**
- **Beschränkung der Weitergabe**
- **festgelegte Speicherzeit**
- **klare Zuständigkeit + Instanzenwege**
- **Verständlichkeit**
- **Bekanntheit + Einhaltung (z.B. Schulungen, Audits,...)**

Es gibt vieles,

für das es sich lohnt,

organisiert zu sein.